EXHIBIT 13

A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It

Orin S. Kerr*

Introduction

The privacy of stored Internet communications in the United States is governed by a federal statute known as the Stored Communications Act ("SCA").[1] The SCA was enacted in 1986 as part of the Electronic Communications Privacy Act.[2] Despite its obvious importance, the statute remains poorly understood. Courts, legislators, and even legal scholars have had a very hard time making sense of the SCA.[3] The statute is dense and confusing, and few cases exist explaining how the statute works.[4] The uncertainty has made it difficult for legislators to legislate in the field, reporters to report about it, and scholars to offer scholarly guidance in this very important area of law.

This Article presents a user's guide to the SCA. My primary goal is to explain the basic structure and text of the Act so that legislators, courts, academics, and students can understand how it works—and in some cases, how it doesn't work. I hope to explain the nuts and bolts of the statute's many distinctions and dichotomies to reveal both the statute's dynamics and its drafters' choices. I will suggest that the statute works reasonably effectively, although certainly not perfectly. The SCA is a bit outdated and has several gaps in need of legislative attention, but by and large it reflects a sound approach to the protection of stored Internet communications. I will also explore some of the present controversies that surround how best to interpret the SCA. In particular, the recent United States Court of Appeals for the Ninth Circuit decision in *Theofel v. Farey-Jones*,[5] offers a new view of the SCA's basic structure that is quite different from the traditional understand-

* Associate Professor, The George Washington University Law School.

1 *See* 18 U.S.C. §§ 2701–2711 (2000 & Supp. I 2001). The statute has been given various names by different commentators. Its names have included: (1) the "Electronic Communications Privacy Act" or "ECPA" because it was first enacted as part of that statute; (2) "Chapter 121" because it has been codified in Chapter 121 of Title 18 of the United States Code; (3) the "Stored Wired and Electronic Communications and Transactional Records Access" statute or "SWECTRA" because that is the formal title given to Chapter 121 in Title 18; and (4) "Title II" because it was enacted as the second title of ECPA. For reasons too complicated and uninteresting to explain here, I find it easiest and simplest to refer to the statute as simply the Stored Communications Act, or "SCA."

2 *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

3 *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 820–21 (2003) (citing cases).

4 *See id.* at 821–26 (discussing the number of cases interpreting the SCA and explaining how the paucity of case law derives from the absence of a statutory suppression remedy).

5 Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

vacy."[120] The court rejected the argument that the emergency exception of § 2702(c)(4) applied: AOL's disclosure was not on its own initiative, the court noted, but was triggered by the officers' request.[121] Although *Freedman* leaves many issues unanswered,[122] it suggests that disclosures will be presumed to fall under § 2703 unless an exception under § 2702 is affirmatively established.

B. Providers "To The Public" Versus Nonpublic Providers

The second critical distinction drawn by the SCA is the line between providers that make their services available "to the public" and those that do not. The distinction is important both for compelled and voluntary disclosure rules. In the case of voluntary disclosure rules, the distinction is critical; the SCA's voluntary disclosure limitations apply only to providers that make services available to the public.[123] As a result, the public/nonpublic line is generally the first inquiry when evaluating the legality of a voluntary disclosure. The distinction also carries importance in the compelled disclosure rules through the definition of RCS. Because an RCS by definition must provide services to the public,[124] opened e-mail held by a provider is protected by the RCS rules if it provides services to the public, but it is not protected by the SCA at all if it does not.

Fortunately, the legislative history of the SCA and a few cases on the question indicate a fairly clear line between the two categories. A provider "to the public" makes its ECS or RCS services available to the public at large, whether for a fee or without cost.[125] For example, a commercial ISP such as America Online or Comcast is available to the public: anyone can sign up and pay for an account. On the flip side, providers do not provide services to the public if its ECS or RCS services are available only to users with special relationships with the provider.[126] If a university provides accounts to its faculty and students or a company provides corporate accounts to its employees, those services are not available to the public.[127] In these contexts, the provider offers the user an account because the provider has a special relationship with the user.

Why does the SCA draw such an important distinction between public and nonpublic providers? The legislative history is not clear on this question, but two plausible explanations exist. First, the law may afford less protection to accounts with nonpublic providers because nonpublic accounts may exist more for the benefit of providers than for the benefit of users. For example, companies often provide e-mail accounts to employees for work-related pur-

---

120 *Id.* at 126.

121 *See id.* at 128.

122 *See, e.g., id.* ("The Court declines to speculate whether it would ever be appropriate . . . for the government to notify the ISP of an emergency and receive subscriber information without conforming to the ECPA."). By "the ECPA," the court was presumably referring to § 2703.

123 *See* 18 U.S.C. § 2702 (2000).

124 *See* 18 U.S.C. § 2711(2) (2000 & Supp. I 2001).

125 *See* Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1042–43 (N.D. Ill. 1998).

126 *See id.* at 1043.

127 *See id.*

poses; the U.S. military often provides accounts to service members for official government business. These nonpublic providers generally have a legitimate interest in controlling and accessing the accounts they provide to users. Plus, their users tend to recognize that the providers will view those provider interests as more important than the privacy interests of users.

In contrast, an individual who contracts with a commercial ISP available to the public usually does so solely for his own benefit. The account belongs to the user, not the provider. As a result, the user may understandably rely more heavily on the privacy of the commercial account from the public provider rather than another account with a nonpublic provider. Many Internet users have experienced this dynamic. When an e-mail exchange using a work account turns to private matters, it is common for a user to move the discussion to a commercial account. "I don't want my boss to read this," a user might note, "I'll e-mail you from my personal account later." The law recognizes this distinction by drawing a line between accounts held with public and nonpublic providers. In practice, the public/nonpublic line often acts as a proxy for the distinction between a user's private account and one assigned to him by his employer.[128]

A related explanation for this distinction is that private providers with a relationship to their users may approach their users' privacy differently than would commercial providers available to the public. To a commercial ISP, a particular customer is a source of revenue, no more and no less. In contrast, nonpublic providers may have a long-term, multifaceted relationship with their users, giving nonpublic providers unique incentives to protect the privacy of their users. The law may wish to protect privacy more heavily in the case of public providers because there is less incentive for public providers to protect their users' privacy. Alternatively, the law may take a more hands-off approach with respect to nonpublic providers in recognition of the different relationships that nonpublic providers may have with their users.

C. Content Information Versus Noncontent Information

The SCA also draws an important line between "contents" of communications and noncontent information—or as the statute labels it, "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)."[129] Compelled disclosure of content information is regulated by § 2703(a) and § 2703(b),[130] while compelled disclosure of noncontent information is covered by § 2703(c).[131] Similarly, voluntary disclosure of contents is regulated by § 2702(b),[132] while

---

128 Network accounts at educational institutions present a potentially troubling exception. Educational institutions often provide Internet accounts to their students, and students often use those accounts as primary, private accounts. Such providers, however, do not provide services to the public.

129 18 U.S.C. § 2703(c)(1) (2000 & Supp. I 2001).

130 *See id.* § 2703(a), (b).

131 *See id.* § 2703(c).

132 *See id.* § 2702(b).